УДК 343.352

П. Д. Біленчук
кандидат юридичних наук, доцент, професор

Київський університет права НАН України

Л. В. Борисова
кандидат юридичних наук, доцент

Національний університет цивільного захисту

В. П. Колонюк
кандидат юридичних наук, доцент,
учений секретар

Київський науково-дослідний інститут судових експертиз
Міністерства юстиції України

КОНЦЕПТУАЛЬНІ ОСНОВИ МІЖНАРОДНОЇ ТА РЕГІОНАЛЬНОЇ ЮРИСДИКЦІЇ ІНФОРМАЦІЙНОГО ПРАВА З ПРОТИДІЇ КІБЕРЗЛОЧИНАМ

У даній статті здійснено аналіз основних міжнародних документів, які забезпечують правове регулювання інформаційних технологій, зроблено висновок, що кінцевою метою кожного комп'ютерного злочину є отримання інформації, яка зберігається, передається, обробляється на комп'ютері в будь-якому вигляді (закодована або ні) та вміщує дані про сфери людської діяльності, а також запропоновані шляхи для ефективної діяльності по розслідуванню транснаціональних комп'ютерних злочинів.

Аналізуючи та оцінюючи небезпеку протиправних діянь для світового співтовариства як відображення об'єктивної дійсності та міжнародної практики запобігання і протидії, вчені прийшли до висновку, що кількість діянь, які сприймаються міжнародною спільнотою злочинами в XXI столітті, збільшилася. У 20-х роках XX століття частина юристів-міжнародників [1] виступала за прийняття міжнародного кодексу, де були б перелічені найбільш серйозні порушення міжнародного права і встановлені санкції за діяння, що мають ознаки міжнародної суспільної загрози з їхнім поділом на дві групи: міжнародні злочини і «правопорушення міжнародного характеру, стосовно яких має місце конфлікт національних юрисдикцій або складно визначити територіальну юрисдикцію певних держав». Міжнародна конференція по уніфікації кримінального законодавства, яка проходила у 1927 році у Варшаві, до міжнародних злочинів віднесла такі правопорушення: 1. Піратство. 2. Підробка металевих грошей і державних цінних паперів. 3. Торгівля рабами. 4. Торгівля жінками і дітьми. 5. Навмисне застосування будь-яких засобів, що здатні спричинити суспільну небезпеку. 6. Торгівля наркотиками. 7. Торгівля

порнографічною літературою [2, с. 13]. 8. Інші злочини, які передбачені міжнародними конвенціями» .

Глобальний кримінальний світ, як і вся світова спільнота, здійснює свою еволюцію і на цьому процесі позначаються такі суттєві чинники:

– технологічні — впливаючи на розвиток світу в цілому, вони видозмінюють і злочинне середовище відносно різних сфер діяльності, наприклад, від підробки комп'ютерних дисків до виробництва синтетичних наркотиків;

– політичні — вважається, що на базисному рівні злочинні діяння визначаються законами, а закони формулюються державою. Адольф Кетле в своїй праці «Соціальна система и закони які нею управляють» визначив: «що число злочинів залежить не тільки від моральних цінностей особистості, але і від соціальних умов, в яких він знаходиться, але також від законів, які повинні гармонійно узгоджуватися з устоями і потребами народів. Відсутність цієї гармонії частіше всього породжує громадські безпорядки» [3, с. 218];

– економічні чинники — організована злочинність (транскордонна, транснаціональна, трансконтинентальна, планетарна) дуже чутлива до економічного середовища;

– чинники, які пов'язані з правоохоронною діяльністю: успішні дії правоохоронців спричиняють неочікувані наслідки — злочинні структури стають більш обережними;

– внутрішні чинники, що формують злочинний світ, як дають змогу уникнути конфліктів і зробити дії злочинців більш ефективними, так й спричиняють ворожнечу і конкуренцію.

Таким чином, в умовах новітніх технологій в усіх сферах життя людини і постійно наростаючої взаємозалежності членів міжнародного співтовариства, «практично всі злочини, які передбачаються загальним кримінальним правом, мають міжнародну направленість» [4, с. 217], зовнішні риси і змістовні ознаки яких не можуть бути вичерпаними — уточнюється їхня система, вдосконалюються і розвиваються правові норми.

Різним аспектам комп'ютерної злочинності, способам і механізму їх вчинення, технології та техніці виявлення і закріплення слідів, тактиці проведення слідчих дій приділялася увага в наукових працях вітчизняних і зарубіжних вчених: В. Г. Афанасьєва, Ю. М. Батуріна, В. П. Бахіна, Н. Вінера, В. Б. Вєхова, А. Б. Венгерова, О. А. Гаврилова, В. О. Голубєва, М. В. Гуцалюка, І. З. Карася, В. В. Крилова, В. Д. Курушина, В. О. Мещерякова, М. С. Полєвого, В. Ю. Рогозіна, М. Г. Шурухнова. Теоретичним підґрунтям дисертаційних досліджень які здійснюються в Україні, стали роботи вчених: Р. С. Бєлкіна, В. І. Галагана, І. Ф. Герасимова, В. Г. Гончаренка, Л. Я. Драпкіна, А. В. Іщенка, Н. І. Клименко, В. В. Клочкова, М. В. Костицького, В. О. Коновалової, В. С. Кузьмічова, В. Г. Лукашевича, В. К. Лисиченка, Є. Д. Лук'янчикова, О. Є. Манохи, Г. А. Матусовського, Л. С. Митричева, В. О. Образцова, М. В. Салтевського, М. Я. Сегая, О. Г. Філіппова, М. В. Терзієва, В. В. Тіщенка, В. Ю. Шепітька, М. П. Яблокова та інших.

Метою статті є потреба у подальшому поглибленому дослідженні міжнародної та регіональної юрисдикції інформаційного права кіберзлочинності, з метою підсилення ефективності боротьби запобігання і протидії протиправним діям в сфері інформаційних технологій.

Злочини міжнародного характеру, до яких відносяться діяння, що «посягають на інтереси декількох держав, які вчиняються особами (групами осіб) не у зв'язку з політикою будь-якої держави» [5, с. 116], а всупереч законодавству і правопорядку своєї держави заради досягнення власних протиправних цілей, також представляють міжнародну суспільну загрозу.

Досягнення в галузі транспорту, зв'язку та інших сучасних технологій, що супроводжуються збільшенням взаємозв'язків і глобалізації соціальної, політичної й економічної систем, викликали відповідні зміни в злочинному середовищі. Здатність злочинних груп розповсюджувати свій вплив за межі національних кордонів і діяти сумісно з правопорушниками у рамках юрисдикції інших держав, дозволяє їм використовувати існуючі в світі диспропорції в пропозиціях, попиті й вартості товарів, обіг яких обмежений з політичних міркувань. Стан охорони національних кордонів і рамки юрисдикції вивчаються зловмисниками, з ціллю укривання доказів та уникнення від розслідування та судового переслідування. Відповідно, можна говорити про транснаціональну злочинність [6, с.160], що відображено в документах Організації Об'єднаних Націй (ООН). Найбільш небезпечною на сьогоднішній день є міжнародна організована злочинність (транснаціональна, транскордонна, трансконтинентальна, планетарна).

Юридичним підґрунтям відповідальності за злочини міжнародного характеру є міжнародні конвенції по запобіганню і протидії конкретним видам злочинів і прийняті у відповідності з ними національні норми кримінального права [7, с. 284]. Укладаючи міжнародні конвенції, держави світу в процесі співробітництва вирішують наступні завдання [8]:

– узгоджують кваліфікації злочинів, які представляють міжнародну суспільну небезпеку;

– домовляються про включення у національне кримінальне законодавство норм щодо відповідальності за такі діяння і відповідного ступеню тяжкості їхнього покарання;

– встановлюють юрисдикції над злочинами і можливими злочинцями (підозрюваними);

– взаємодіють у процесі здійснення кримінального переслідування, враховуючи надання правової допомоги.

У 90-х роках у зв'язку із зростанням занепокоєння з приводу транснаціональної організованої злочинності був проведений цілий ряд міжнародних (форумів, симпозіумів) нарад, на яких розглядалися можливі рішення цієї проблеми. Поступово склався значний комплекс багатосторонніх міжнародних конвенцій, кожна з яких присвячена певному виду злочинів [9]. Відповіддю міжнародної спільноти глобальному кримінальному світу стала міжна-

родна угода ООН, а саме Конвенції ООН проти транснаціональної організованої злочинності (резолюція 55/25 Генеральної Асамблеї від 15 листопада 2000 року), яка має допомогти державам у вирішенні спільної проблеми і, у відповідності з якою, ці документи не застосовуються у відношенні правопорушень, що не відносяться до організованої злочинності, розглядаючи як виняток тільки окремі сфері — особливо корупцію і комп'ютерні правопорушення, що вчиняються окремими особами і стали проблемою, яка потребує надзвичайно більшої міжнародної уваги. Відомо, що Конвенція застосовується у тих випадках, коли «відповідний злочин повинен мати «транснаціональний характер». Як правило, такими є злочини, які плануються чи вчиняються в кількох державах, або вчиняються в одній державі, а мають істотні наслідки в іншій» [10, с. 45–46].

Даючи визначення держави, як правило, цитують Конвенцію про права і обов'язки держав, яка прийнята на VII Міжнародній конференції американських країн у 1933 році в Монтевідео, у якій йдеться мова про права і обов'язки держав: держава, будучи представником міжнародного права, має право видавати свої закони, управляти, визначати юрисдикцію й компетентність власних служб і організацій та закони, що прийняті в цій державі, є обов'язковими для всіх, хто мешкає на території цієї держави [6, с. 28].

Держава характеризується об'єктивно притаманною їй політико-юридичною властивістю — суверенітетом і «кожна держава зобов'язана поважати суверенітет інших учасників системи, тобто їхнє право в межах власної території здійснювати законодавчу, виконавчу, адміністративну й судову владу без будь-якого втручання з боку інших держав» [12, с. 30].

Принцип «загальної юрисдикції» застосовується для вузької категорії діянь, за вчинення яких законодавчо передбачається переслідування державами, які поділяють цей принцип, незалежно від місця вчинення таких злочинів та їхнього впливу на державу, в якій здійснюється юрисдикція. По-перше, існування різних принципів, більшість із яких заперечують один одного, приводить до думки, що проблеми юрисдикції не нові в сучасному міжнародному праві. Інтернет і комп'ютерні системи тільки розширюють спектр потенціальних проблем. По-друге, належить відмітити очевидне протиріччя «глобалізації» та «безмежності» Інтернет принципам юрисдикції, а це вносить певні зміни в концепції здійснення юрисдикції.

Юридична рівність держав не означає їхньої фактичної рівності, що і враховується в реальних міжнародних відносинах [13, с. 5–12]. У міжнародному праві існує декілька традиційних юридичних норм. У більшості суперечливих випадків рішення, як правило, приймається на користь «територіального» принципу (основа для здійснення свого законодавства) або відповідно до міжнародних угод. Сьогодні може виникнути ситуація, коли спроба однієї сторони визначити правила екстра-територіальної юрисдикції іншої сторони, сприймається як посягання на державний суверенітет. Такими прикладами є спроби однієї держави здійснювати дії, що суперечать місцевому

законодавству або держава визначає кримінальним діяння, що не є таким у відповідності до територіальної юрисдикції.

У тих державах світу, де діє принцип верховенства права і поважають законність, Інтернет — це тільки функція глобальної телекомунікаційної революції. Поки існують великі об'єми даних, які пов'язані з використанням можливостей Інтернету, то ця мережа без сумніву є однією найбільш важливою інформаційною і впливовою мережею світу. Крім Інтернету існує ще безліч приватних спеціалізованих мереж, але, і без їхнього врахування, можна стверджувати, що винайдення модему й міжнародної телефонії означає, що люди, які працюють за комп'ютером в одній державі, можуть мати необмежений вплив на роботу комп'ютерів у інших державах.

Підсумовуючи результати Всесвітнього наукового форуму, який відбувся у Будапешті з 8 по 10 листопада 2003 року, генеральний секретар Угорської академії наук Норберт Кро, навів слова історика науки Ричарда Ослона: «Без науки мораль сліпа, але без моралі наука безкорислива, беззмістовна і безсила» [14, с. 76]. Науково-технічний прогрес поставив перед людством серйозні проблеми і встановив колосальну відповідальність за використання отриманої могутності: «розвиток техніки несе необмежені можливості для добра і зла» [15, с. 166]. Кібернетика, інформатики і робототехніка стала фактором кризи, сприяючи другій промисловій революції.

Таким чином, проблеми, які ставляться сучасними технологіями, можуть вирішуватися за допомогою тих самих технологій. І, відповідно, поняття територіальності може стати фундаментальним у формуванні концепції «кіберправа», «кібербезпеки», «кіберкриміналістики». Експерти в галузі інформатики відмічають: «інформаційне суспільство» не має політичних, соціальних та економічних кордонів [17, с. 188]. Транснаціональний характер злочинності з використанням телекомунікаційних мереж дає змогу вважати, що розробка загальної політики з ключових питань повинна бути частиною будь-якої стратегії в боротьбі зі злочинністю. Така концепція має важливе значення для запобігання виникнення «інформаційних сховищ», у тому числі й в рамках тих правових систем, де комп'ютерні злочини не є кримінально карними. Разом з тим, принцип державного суверенітету, залишається нездоланною перешкодою, так як потенційно будь-яка держава може надати притулок екстремістам, злочинцям, фальшивомонетникам або терористам. Боротьба зі злочинністю в сучасних умовах широкого використання міжнародних телекомунікаційних мереж ускладнюється з таких причин:

– відкриті структури телекомунікаційних мереж дають користувачам таке правове середовище, яке оптимально відповідає їхнім цілям, тобто користувачі можуть вибирати держави, в яких певні дії, вчинені в електронному середовищі, не спричиняють кримінальної відповідальності порівняно з їхнім внутрішнім правом;

– для розслідування злочинів, що мають місце в електронному середовищі, потрібен спеціальний досвід і знання, належні правові процедури роз-

слідування й юридичні повноваження, якими правоохоронні органи відповідних держав можуть не володіти;

– у той же час слідчі дії правоохоронних органів у цілому повинні обмежуватися територією власної держави, а це означає, що для боротьби зі злочинами у відкритих телекомунікаційних мережах необхідно активізувати міжнародне співробітництво.

У 1994 році Радою Європи був прийнятий знаковий документ Banqemann Report, який намітив у загальних рисах Європейську політику щодо інформаційної безпеки в мережі Інтернет, які характеризуються як пріоритетні та такі, що вимагають негайних дій. Європейська Комісія стала брати більш активну участь у вирішенні проблем, пов'язаних із комп'ютерними злочинами після інституційних змін, внесених Амстердамською угодою 1997 року, яка модифікувала Римську угоду — основоположний документ Європейського Союзу і забезпечила загальну політику щодо запобігання та протидій транснаціональній кримінальній діяльності.

У 1998 році Європейська Комісія заключила з містом Вюрцбургом (ФРН) контракт, який передбачає складання соціально правових документів в процесі здійснення слідчих і судових процесуальних дій при розслідуванні комп'ютерних злочинів. Фундаментальний правовий документ, відомий як дослідження Comcrime Study, закликає до правової гармонізації, спеціальної підготовки правоохоронних органів і судового персоналу, а також до міжнародної кооперації.

У жовтні 1999 року на Саміті в місті Тампері члени Європейського Союзу вирішили включити високотехнологічні комп'ютерні злочини, як одну із важливих сфер для загально визнаних аналітичних правових підходів і санкцій. Європейська комісія має спеціального на меті створення спеціальної поліції з розслідування комп'ютерних злочинів на національних рівнях, особливо в тих державах, де така поліція не існує чи не має законодавчого урегулювання, відповідного технічного обладнання й організаційного досвіду, а також координування діяльності з іншими міжнародними інститутами, такими як Рада Європи і «Велика вісімка».

У січні 2001 року Європейська комісія опублікувала давно очікуваний план боротьби з комп'ютерним шахрайством, у якому особлива увага приділяється правопорушенням, що пов'язані з несанкціонованим доступом, саботажем і порушенням прав інтелектуальної власності, незаконними або расистськими повідомленнями. У цьому документі пропонується гармонізувати правові процедури, звертається увага на проблеми законного перехоплення телекомунікацій та доступу до потоків даних з боку операторів мережі / постачальників послуг мережі системи Інтернет з урахуванням інтересів останніх і правоохоронних органів, з одночасним дотриманням принципів приватності та конфіденційності в питаннях стосовно персональних даних.

Комітет експертів з кіберзлочинів (Committee of Experts on Crime in Cyber-Space), який був організований за рішенням Ради Європи в 1996 році, у

вересні 2001 року надав для затвердження Комітету міністрів остаточну — двадцять восьму версію Конвенції щодо комп'ютерних правопорушень, в якій досить чітко визначені види комп'ютерної злочинності та шляхи взаємодії урядів щодо боротьби з комп'ютерними правопорушеннями.[17]

Постає складною задачею визначення сфери дії, розповсюдження та збитків від комп'ютерних злочинів, які вчиняються в інформаційному просторі. Вивчення цих проблем дозволило зробити висновок, що «кінцевою метою кожного комп'ютерного злочину є отримання інформації, яка зберігається, передається, обробляється на комп'ютері в будь-якому вигляді (закодована або ні) та вміщує дані про сфери людської діяльності» [18, с. 24]. У грудні 2000 року міністр внутрішніх справ Великої Британії заявив про 50% зростання комп'ютерних злочинів. Служба комерційних злочинів Міжнародної торгової палати (The International Chamber of Commerce (ICC) розглянула більш, ніж 2000 випадків шахрайства з використанням мережі Інтернет. [19, с. 18] За даними інституту комп'ютерної безпеки (Computer Security Institute), кількість хакерських атак у світі в другій половині 2002 року збільшилася на 32 % у порівнянні з відповідним періодом 2001 року. Згідно зі статистичними даними аналітиків компанії Internet Security System, яка відома своїми дослідженнями в галузі електронної безпеки, кількість комп'ютерних інцидентів у світі збільшилася на 15 % у третій чверті 2003 року.

Розробка загальної політики по протидії кіберзлочинності стала одним із напрямів діяльності Програми ООН. Метою керівного документу із запобігання злочинам, пов'язаних із використанням комп'ютерів і боротьбою з правопорушеннями в сфері інформаційних технологій, опублікованого Організацією Об'єднаних Націй, є узгодження як матеріального, так і процесуального права, а також міжнародне співробітництво в боротьбі зі злочинністю, пов'язаною з використанням комп'ютерів. У зв'язку з цим звертається особлива увага світової спільноти на такі важливі аспекти [20, с. 2]:

– сприяння розробці правотворчими органами стандартів для забезпечення надійності та безпеки телекомунікацій та технологій обробки даних;

– розробка інформаційних і телекомунікаційних систем, здатних виявляти зловживання в мережах, відслідковувати осіб, які вчиняють такі зловживання й збирати відповідні докази.

Практично до останнього часу співробітники правоохоронних органів багатьох країн світу були далекі від розуміння того, що новітні комп'ютерні технології є революційними в діяльності злочинного світу.

У грудні 2002 року в Лондоні відбувся Перший міжнародний стратегічний конгрес «E-CRIME CONGRESS 2002», присвячений співробітництву між правоохоронними структурами різних держав світу, підготовлений і проведений Національним центром по боротьбі зі злочинами в сфері високих технологій (National Hi-Tech Crime Unit — NHTCU). У роботі конгресу «E-CRIME» взяли участь близько 400 делегатів, які представляли державні, комерційні, наукові та правоохоронні органи; делегатів репрезентували МВС

Великої Британії, Інтерпол, Європол, ФБР, Україна, Управління «Р» (Росія), Microsoft, Symantec, IBM, Sun Microsystems Ltd., VISA, Master Card, eBay, Bank of New York, Swedbank та інші. На засіданнях були оголошені такі факти: 90% організацій виявляють порушення інформаційних систем щороку; 80% із них підтверджують фінансові збитки (тільки один вірус NIMDA спричинив збитки на 1,8 млрд. фунтів); щороку викрадається приватної інформації на суму понад 38 млрд. фунтів. Учасники даного Конгресу наголосив, що Інтернет дає змогу організованим злочинним групам, знаходячись у мережі, порушувати закон на відстані, швидко й незалежно від громадянства і місця перебування. Наприклад, за повідомленнями інформаційного агентства Washington Pro File, терорист Усама Бен Ладен одержав комп'ютерну програму Promis (компанія Inslaw Inc.,), за допомогою якої можна проникати в урядові інформаційні мережі США, стежити за діями американських спецслужб, одержувати таємну інформацію про стратегічні об'єкти США, без проблем відмивати брудні гроші. Зазначимо, що ці програми, створені на базі розробок Inslaw Inc., використовуються ФБР, ЦРУ, США.

Визнаючи загрозу безпеці та добробуту народів світу, яку несе в собі транснаціональна комп'ютерна злочинність, Україна на Саміті тисячоліття у вересні 2000 року виступила з ініціативою про розроблення Міжнародної Конвенції по боротьбі з комп'ютерним тероризмом [21, с. 5–12].

Іншою важливою міжнародною проблемою на сьогоднішній день є спам — масова несанкціонована розсилка електронних повідомлень рекламного чи іншого характеру, або «захламлення» електронної поштової адреси (адрес) значною кількістю повідомлень, що призводить до модифікації вмісту поштових скриньок потерпілих, а у випадку переповнення їх спамом до блокування надходження повідомлень.

Аналітики відмічають не тільки кількісний, але й якісний розвиток спама. Підтвердилися прогнози щодо розповсюдження політичного спама. Поштова служба «Яндекса» повідомила, що доля спамерських листів у поштових потоках складає 40%, при цьому загальний об'єм масової небажаної кореспонденції складає 60–80%. За даними поштових служб «Рамблера» і «Mail.ru.», спам сьогодні займає до 80% поштового трафіка. У 2003 році було вчинено чотири зовсім нові, потужні, непередбачені Інтернет-атаки. 2003 рік змусив усіх по-новому подивитися на проблему спама: з'явилися шкідливі програми, що успішно використовують спам-технології. Спам — прибутковий бізнес і в майбутньому спамерський бізнес, уже визнаний незаконним у більшості держав світу, буде контролювати мафія, представники якої в мережі Інтернет будуть виконувати функції податкової поліції, що створює загрозу безпеці мереж як у національному, так і в світовому масштабі. Одним із шляхів вирішення проблеми бачиться в обов'язковій авторизації користувачів мережі та створення Інтернет-поліції або е-Інтерполу. Наприклад, американським сенатом схвалено законопроект, згідно з яким на будь-яке несанкціоноване рекламне повідомлення накладається штраф у межах 1 млн.

доларів США. Одночасно користувачі, які постраждали від отримання спаму, можуть вимагати від відправника компенсації за завдану шкоду в розмірах до 200 тис. доларів США за кожний день отримання «сміттєвих» повідомлень [22, с. 106].

Приклад епідемії Slammer показав, що шкідлива програма може порушити цілісність Всесвітньої мережі, а при необхідності відключити національний сегмент Інтернет.

До масштабної програми боротьби із творцями шкідливих програм, яку розгорнула найбільша американська корпорація в галузі програмного забезпечення «Microsoft», до якої приєднався також й Інтерпол. Її спеціальний підрозділ по боротьбі зі злочинами в галузі високих технологій вже почав активно виявляти осіб, які створюють такі програми і розповсюджують їх в Інтернеті. Одночасно Інтерпол розробляє положення про великі грошові премії тим, хто допомагатиме виявляти творців та розповсюджувачів цих шкідливих програм, що призводять до глобальних комп'ютерних збоїв [23, с.11].

Організація боротьби азіатсько-тихоокеанської робочої групи з комп'ютерною злочинністю, моделлю для якої послужила діяльність аналогічної групи в Європі, стала важливим кроком у боротьбі з комп'ютерними злочинами. У жовтні 2000 року Росія, Китай, Південна Корея і Японія домовилися про співробітництво в боротьбі з міжнародними, в тому числі комп'ютерними злочинами [24, с.10]. Створення в Китаї «поліції антивіруса» засвідчило той факт, що ці держави дійсно розуміють небезпечний розвиток комп'ютерних злочинів як реальну загрозу національній безпеці.

Упродовж останніх років правоохоронні органи багатьох країн світу почали накопичувати власний правовий і технічний досвід для боротьби з комп'ютерними злочинами. Як підкреслює англійський криміналіст М. А. Уілмер, «злочинці та працівники органів кримінальної юстиції ведуть між собою постійну боротьбу за інформацію» [25, с. 27].

У ряді держав світу вже підготовлені керівні правові нормативні документи, що вміщують технічні та процесуальні інструкції стосовно напрямів проведення розслідування, а це дозволяє скоротити об'єм втрачених доказів і забезпечити їхню допустимість використання в суді. У відомчих структурах Інтерполу створено декілька робочих груп експертів зі злочинності, пов'язаної з інформаційними технологіями, які займаються розробкою конкретних засобів програмного забезпечення з метою виявлення визначених злочинів у Інтернет. Наприклад, Європейська робоча група розробила керівний нормативний документ по розслідуванню комп'ютерної злочинності (існує на CD-ROM), де вміщуються інструкції з методики розслідування випадків, пов'язаних із комп'ютерною злочинністю, описання засобів і методів пошуку й захисту електронних матеріалів, а також інформацію про відповідні матеріальні та процесуальні правові норми різних держав світу. Для зменшення часу реагування, пов'язаного з ідентифікацією правопорушника, агентство оборонних інформаційних систем DISA (Defense Information Systems Agency) намагається

скоротити час реакції з чотирьох годин до чотирьох секунд, що дасть змогу вирішити одну із головних проблем відстеження комп'ютерних посягань, а саме, виявлення джерела вторгнення по телекомунікаційній мережі. DISA вже започаткувало систему аналізу вторгнень по мережах у не таємний протокол маршрутизації в мережі Інтернет [26, с. 16].

Міжнародна Торгова Палата (ICC) організувала спеціальний відділ для захисту 7000 компаній в усьому світі від комп'ютерних злочинів. Крім визначення методів здійснення атак, відділ надає спеціальну інформацію про захист від атак. Також розвивається спеціальна база даних про кримінальні дії в інформаційному просторі та налагоджується співробітництво між правоохоронними органами і недержавними організаціями. У Рекомендаціях Ради Європи (R(89)9, R(95)13) підкреслюється необхідність створення в рамках національних правоохоронних органів спеціалізованих підрозділів з проблем запобігання і протидії комп'ютерній злочинності. Такі підрозділи необхідно забезпечити відповідними законами, нормативними актами, укомплектувати підрозділи кіберполіції професійно високо підготовленими кадрами, оснастити відповідним технологічним обладнанням і засобами програмного забезпечення.

Із урахуванням існуючих сьогодні в світі міжнародних масштабів телекомунікаційних мереж менш ймовірним стає те, що всі елементи кіберзлочинності будуть обмежені територією однієї держави. У залежності від відношень між зацікавленими державами, характеру відповідної інформації та інших факторів може виникнути потреба в розробці повноважень і процедур у спеціальних міжнародних угодах. [27, с.169]. У сучасному міжнародному праві сьогодні існує поняття саме обов'язку держав співпрацювати один з одним і ООН. До 1945 року співробітництво окремих держав у світі залежало від їхньої доброї волі, але з прийняттям Уставу ООН у міжнародну практику ввійшов новий принцип співробітництва держав: «по-перше, підтримувати мир і безпеку можна лише шляхом співробітництва в різних сферах міжнародного життя; по-друге, сучасні проблеми настільки ускладнилися, що поодинці вирішувати їх вже практично неможливо» [28, с. 69].

Здійснення згідно зі статтями Європейської Конвенції про взаємну допомогу в кримінальних справах між державами-членами Європейського Союзу [29] спільних дій, при розслідуванні транснаціональних комп'ютерних злочинів ускладнюються з таких причин:

– традиційні форми співпраці передбачають письмові клопотання про надання правової допомоги, а це пов'язано з втратою часу у випадку розслідування комп'ютерних злочинів, що спричиняє втрату доказів внаслідок знищення «історичних даних»;

– виявлення, закріплення, вилучення і дослідження «історичних даних», збережених за допомогою комп'ютерних мереж є можливим стосовно двох держав (держави місця знаходження потерпілої особи і держави, в якій перебуває злочинець). Якщо комп'ютерне повідомлення проходить через три і

більше держав, то надання правової допомоги може затягнутися на тривалий час, у результаті чого існує значна ймовірність зміни чи знищення «історичних даних»;

– законами одних держав проводиться розмежування між пошуком і перехопленням даних у процесі їхньої передачі та пошуком даних, що зберігаються, в той час як у правових системах інших держав чітке розмежування відсутнє.

Входження України до Європейського співтовариства та підписання нашою державою 23 листопада 2001 року Європейської Конвенції про кіберзлочинність, в якій визначені конкретні шляхи взаємодії урядів щодо боротьби з ними, сприяло розробці концепції реформування взаємодії правоохоронних органів України з правоохоронними органами зарубіжних країн.

Аналіз основних міжнародних документів правового регулювання інформаційних технологій дозволив зробити висновок про те, що для ефективної діяльності з метою розслідуванню транснаціональних комп'ютерних злочинів необхідно:

– ***здійснити*** уніфікацію кримінального й кримінально-процесуального законодавств кожної держави за вчинення комп'ютерних злочинів;

– ***усунути*** норми «подвійного права»;

– ***удосконалити*** протокол офіційної правової допомоги для ефективного розслідування злочинів і вирішення проблеми оперативного отримання із-за кордону вилучених й збережених на час надання правової допомоги комп'ютерної інформації в документованому виді для використання як доказу;

– ***передбачити*** канал зв'язку для забезпечення обслуговування невідкладних запитів у будь-який проміжок часу в усіх часових поясах з метою удосконалення системи слідчих і оперативно-розшукових заходів, особливо стосовно кримінальних проваджень, які торкаються інтересів декількох держав;

– ***запровадити*** системи ідентифікації для сприяння пошуку комп'ютерного злочинця за декілька секунд з метою отримання незаперечних доказів його злочинної діяльності;

– ***забезпечити*** обмін адресами операторів мережі/постачальників послуг мережі [31, с. 292].

Перелік посилань

1. *Наприклад*, професор Пелла, організатор і керівник унікального руху, наполягав на віднесенні піратства і підробки грошей і т.п. до «міжнародних злочинів».
2. *Трайнин А. Н.* Защита мира и борьба с преступлениями против человечества. Москва, 1956. С. 13.
3. *Кетле А.* Социальная система и законы ею управляющие / с фр. пер. князь Л. Н. Шаховской. Санкт-Петербургъ. С. 218.
4. *Международное* уголовное право: учеб. пособ. / под общ. ред. В. Н. Кудрявцева.2-е изд. перераб. и доп. Москва, 1999. С. 217.
5. *Транснаціональні злочини* (злочини міжнародного характеру) — це діяння, які передбачені міжнародними угодами, не відносяться до злочинів проти людства, миру і безпеки, але роблять замах на нормальні стабільні відношення між державами,

наносять збитки мирному співробітництву в різних областях відносин (економічній, соціально-культурній, майновій тощо), а також організаціям і громадянам, що караються згідно нормам, встановленим в міжнародних угодах, або згідно нормам національного кримінального законодавства у відповідності з цими угодами. До них відносяться: діяння проти стабільності міжнародних відносин (тероризм, захоплення заручників, захоплення і крадіжку повітряних суден, ін.); діяння, що наносять втрати економічному, соціальному і культурному розвитку держав (виготовлення фальшивих грошей, незаконний обіг наркотиків, легалізація злочинних доходів, др.); злочини, вчинені у відкритому морі; злочинні посягання на особисті права людини (работоргівля, др.) і ряд інших. *Международное право*: учеб. для вузов / Г. В. Игнатенко, В. Я. Суворова, И. О. Туинов и др.; под ред. Г. В. Игнатенко. 2-е изд., перераб. и доп. Москва, 1995. С. 116.

6. *Международное* право: учеб. для вузов / Г.В. Игнатенко, В.Я. Суворова, И. О. Туинов и др.; под ред. Г. В. Игнатенко. 2-е изд., перераб. и доп. Москва, 1995. 399 с.;
7. Там само. С. 160.
8. Там само. С. 284.
9. *До них відносяться* Всесвітня конференція на рівні міністрів по транснаціональній організованій злочинності, яка відбулася у Неаполі, Італія, 21–23 листопада 1994 року (документ A/49/748); Регіональний семінар на рівні міністрів по заходам у зв'язку з Політичною декларацією і Глобальним планом дій проти організованої транснаціональної злочинності, що відбувся у Буенос-Айресі 27–30 листопада 1995 року (документ E/CN.15/1996/2/ Add.1); Регіональній семінар на рівні міністрів держав Африки по організованій транснаціональній злочинності та корупції, що проходив у Дакарі 21–23 липня 1997 року (документ E/CN.15/1998/6/Add.1); Регіональний семінар на рівні міністрів країн Азії по організованій транснаціональній злочинності та корупції, який відбувся у Мілані 23-25 березня 1998 року (документ E/CN/151998/6/Add.2) та ін.
10. *Див.*: http: //www/odccp.org/palermo/convmain.html.
11. *Туском Ж.* Міжнародне право: підруч.: пер. з франц. Київ, 1998. С. 45–46.
12. *Международное право*: учебник / отв. ред. Ю. М. Колосов, В. И. Кузнецов. (Дипломат. акад. МИД РФ, МГИ МО МИД РФ). Москва, 1996. С. 28.
13. Там само. С. 30.
14. *Наука и политика*: место встречи — Будапешт // Наука и жизнь. 2004. № 1. С. 5–12.
15. *Винер Н.* Кибернетика или управление и связь в животном и машине: пер. с англ. / предисл. Г. Н. Поварова. 2-е изд. Москва, 1968. С. 76.
16. *Международное* право: учебник / отв. ред. Ю. М. Колосов, В. И. Кузнецов. Москва, 1996. С. 166.
17. *Breivik P. S.* Education for the information age / D. W. Farmer, T. F. Mech, eds. // New Directions for Higher Education. 1992. № 78.
18. *Черних А. В.* Обеспечение безопасности автоматизированных информационных систем (уголовно-правовые аспекты) // Советское государство и право. 1990. № 6. С. 118.
19. *Инициативы* Европейской Комиссии по борьбе с преступностью // Проблемы преступности в капиталистических странах. Москва, 2002. № 8. С. 24.
20. *Преступления*, связанные с использованием компьютерной сети: справ. док. для семинара-практикума по использов. компьютерной сети // Десятый Конгресс ООН по предупреждению преступности и обращению с правонарушителями: док. ООН A/CONF/187/10. С.18.
21. *Виступ Президента* України Леоніда Кучми на пленарному засіданні Генеральної асамблеї ООН // Крок. 2000. № 17–18. С. 2.
22. *Наука и политика*: место встречи — Будапешт // Наука и жизнь. 2004. № 1. С. 5–12.

23. *Интерпол* против вирусов // Наука и жизнь. 2004. № 2. С. 106.
24. *Проблемы киберпреступности* в азиатских странах // Борьба с преступностью за рубежом (по материалам зарубежной печати). Москва, 2002. № 11. С. 11.
25. *Уилмер М. А.* Преступность и теория информации: пер. с англ. Москва, 1973. С. 10.
26. *Некоторые* факты из области киберпреступности // Борьба с преступностью за рубежом (по материалам зарубежной печати). Москва, 2002. № 9. С. 27.
27. *Преступления,* связанные с использованием компьютерной сети: справоч. документ для семинара-практикума по использованию компьютерной сети // Десятый Конгресс ООН по предупреждению преступности и обращению с правонарушителями: документ ООН A/CONF/187/10. С. 16.
28. *Игнатенко Г. В., Суворова В. Я., Туинов И. О.* и др. Международное право: учеб. для вузов. 2-е изд., перераб. и доп. Москва, 1995. С. 160.
29. *Туском Ж.* Міжнародне право: підруч.: пер. з франц. Київ, 1998. С. 69.
30. *Акт Ради* від 29 травня 2000 року про введення в дію Конвенції про взаємну допомогу в кримінальних справах між державами-членами Європейського Союзу відповідно до ст. 34 Договору про Європейський Союз (2000/С 197/01).
31. *У спеціальній* літературі й міжнародних документах відомості про проходження інформації іменуються як «історичні дані», «дані про потоки» або «дані про потоки інформації» і вказують на джерело, призначення, шлях або маршрут,час, дату, розмір, тривалість чи тип мережевого сервісу.
32. *Біленчук П. Д., Гуцалюк М. В., Кравчук О. В., Козир М. В.* Комп'ютерний тероризм: суперхакери, кібер-терористи, кібер-криміналісти: моногр. Київ, 2008. 292 с.

КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ МЕЖДУНАРОДНОЙ И РЕГИОНАЛЬНОЙ ЮРИСДИКЦИИ ИНФОРМАЦИОННОГО ПРАВА ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПЛЕНИЯМ

П. Д. Биленчук
Л. В. Борисова
В. П. Колонюк

В данной статье проведен анализ основных международных документов, которые обеспечивают правовое регулирование информационных технологий, сделано вывод, что конечной целью каждого компьютерного преступления является получение информации, которая хранится, передаётся, обрабатывается на компьютере в любом виде (кодированная или нет) и содержит данные о сферах человеческой деятельности, а также предложены пути эффективной деятельности по расследованию транснациональных компьютерных преступлений.

FUNDAMENTALS OF INTERNATIONAL AND REGIONAL JURISDICTION OF THE INFORMATION LAW ON COOPERATION OF CYBERTRANTS

P. Bilenchuk
L. Borysova
V. Koloniuk

This article analyzes the main international documents of the legal regulation of information technologies and concludes that the ultimate goal of each computer crime is to obtain information that is stored, transmitted, processed on a computer in any form (coded or not) and contains data on spheres of human activity, ways of effective activity on investigation of transnational computer crimes are offered as well.